



Матеріали I Міжнародної науково-практичної конференції «Малинівські читання», м. Острог, 16–17 листопада 2012 року. – Острог: Видавництво Національного університету «Острозька академія», 2012. – С. 243-244.

5. Реалізація нового КПК України у 2013 році (моніторинговий звіт) / О.А. Банчук, І.О. Дмитрієва, З.М. Саїдова, М.І. Хавронюк. – К.: ФОП Москаленко О.М., 2013. – 40 с.

6. Яновська О.Г. Оскарження адвокатою рішень, дій чи бездіяльності слідчого, прокурора та слідчого судді під час досудового розслідування: [наук.-практ. посіб.] / О.Г. Яновська; Академія адвокатури України. – К.: Прецедент, 2013. – 32 с.

7. Узагальнення судової практики оскарження рішень, дій чи бездіяльності під час досудового розслідування у порядку Кримінального процесуального кодексу України, який набрав чинності з 20 листопада 2012 р. – [Електронний ресурс]. – Режим доступу: http://hrga.court.gov.ua/sud2090/inf_court/generalization/criminal11/.

8. Шаренко С.Л. Актуальні питання застосування окремих норм КПК України під час досудового розслідування / С.Л. Шаренко // Право України. – 2013. – № 11. – С. 95-103.

9. Константинов П.Ю. Рассмотрение жалоб на действия (бездействие) дознавателя, следователя и прокурора / П.Ю. Константинов, А.П. Стуканов // Законность. – 2005. – № 6. – С. 17-19.

ПРАВОВАЯ ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ: ЕВРОПЕЙСКИЙ ОПЫТ ДЛЯ УКРАИНЫ НА ОСНОВЕ ПРАКТИКИ РЕСПУБЛИКИ КИПР

Юлия МЕДВЕДЕНКО,

аспирант кафедры правового регулирования экономики
ГВУЗ «Киевский национальный экономический университет имени Вадима Гетьмана»,
юрист юридической компании «Стратег»

Summary

The article analyses leading European experience in measures of prevention of wrongdoings in the field of personal data protection. The difference in approaches and other guidelines to process of bringing to legal responsibility for wrongdoings in area of personal data protection under laws of Republic of Cyprus and Ukraine has been determined. The author exemplifies actual cases of bringing to legal responsibility in specified jurisdictions. Practical recommendations for Ukrainian legislation of personal data protection were offered in order to optimize process of legal training of individuals in mentioned area.

Key words: personal data, legal liability, law of Republic of Cyprus.

Аннотация

В статье анализируется ведущий европейский опыт превентивных мер профилактики совершения правонарушений в сфере защиты персональных данных osoby. Определяется разница в подходах и других ориентирах в процессе привлечения к юридической ответственности за правонарушения в сфере защиты персональных данных по законодательству Республики Кипр и Украины. Автор наводит актуальные ситуации привлечения к юридической ответственности в указанных юрисдикциях. Предлагаются практические рекомендации для законодательства Украины в сфере защиты персональных данных с целью оптимизировать процесс правового обучения физических лиц в указанной сфере.

Ключевые слова: персональные данные, юридическая ответственность, нормы права Республики Кипр.

Постановка проблемы. В условиях стремительного развития информационного пространства, а также трансграничных связей остро встала проблема защиты персональных данных физических лиц не только на локальном, национальном, но и международном уровне. Украина как молодое правовое государство должна ориентироваться и перенимать исключительно качественный и передовой опыт с целью построения собственного института защиты персональных данных. Ярким примером сильной правовой базы и наличия укрепленного мирового авторитета является Республика Кипр. Несмотря на достаточно небольшой промежуток времени с момента принятия законодательства в сфере защиты персональных данных, Кипр получил статус государства, которое умеет и способно защитить данные вверенных лиц.

Актуальность темы исследования подтверждается степенью нераскрыто-

сти темы. На данный момент практически нет фундаментальных работ анализа правовых институтов защиты персональных данных за законодательством Республики Кипр и Украины.

Анализ проблемы правонарушения в сфере защиты персональных данных проводился государственными независимыми органами, такими как комиссар в Республике Кипр и Уполномоченный по правам человека в Украине. Ситуация сложилась так, что несмотря на наличие многочисленных научных трудов в области защиты персональных данных, исследования и правовой анализ соотношения правовых институтов в сфере защиты персональных данных Республики Кипр и Украины отечественными исследователями еще не проводился, что и обуславливает актуальность данного исследования.

Целью и задачей статьи является анализ реального состояния защиты персональных данных по законода-



тельству Республики Кипр и определение характерных особенностей превентивных мер, а также привлечения к юридической ответственности за правонарушения законодательства в сфере защиты персональных данных. Это должно способствовать в принятии положительного иностранного опыта для дальнейшего внедрения в отечественное законодательство. Ведь, несмотря на переживший острый банковский кризис в 2013 году, в связи с чем уменьшился объем прямых инвестиций в экономику Украины, Кипр все равно, согласно данным Государственной службы статистики Украины по состоянию на 01.04.2014 года, остается крупнейшим инвестором – 16 533,60 млн. долл. США (31,7% из общего объема прямых иностранных инвестиций), и государством-партнером [1].

Изложение основного материала. Политика в области защиты персональных данных в Республике Кипр направлена на минимизацию случаев нарушения указанных прав. Как отметил Уполномоченный в сфере защиты персональных данных Республики Кипр, в стране действует постоянная информационная кампания для населения по защите своих персональных данных в целях укрепления правового образования граждан в этой области. Эффективностью проведения вышеуказанной программы является количественный показатель снижения жалоб граждан по вопросам нарушения законодательства в сфере защиты их персональных данных: 2010 год – 804 жалобы, 2011 год – 558 жалобы и соответственно в 2012 году – 142 жалобы [2]. К сожалению, ситуация в Украине выглядит несколько иначе. Согласно информации об обращении граждан к Уполномоченному Верховной Рады Украины по правам человека количество жалоб значительно увеличивается – с 778 в 2009 году до 4130 в 2010 году, где подавляющее большинство верующих граждан жаловалось на нарушение прав по защите их персональных данных [3]. Отделом рассмотрения жалоб, обращений физических и юридических лиц Управления юридического обеспечения Государственной службы Украины по вопросам защиты персональных данных за отчетный период 2012 года было рас-

смотрено 3033 обращения граждан. Из них: 2767 заявлений о рассмотрении вопросов, связанных с обработкой персональных данных и 266 жалоб с требованием о восстановлении нарушенных прав и защиты законных интересов в результате деятельности (бездействия) должностных лиц предприятий, учреждений, организаций [4]. В свою очередь, уже в 2013 году поступило 1039 жалоб и обращений граждан. Характер нарушений законодательства в сфере защиты персональных данных в основном касались: незаконного распространения персональных данных – 109 жалоб, уклонения от регистрации баз персональных данных – 12 жалоб, принуждения к даче согласия на обработку персональных данных – 8 жалоб, отзыва согласия на обработку персональных данных – 15 жалоб, отказа в доступе к собственным персональным данным – 34 жалобы, отсутствия уведомления о включении в базу персональных данных – 28 жалоб, незаконного сбора и использования персональных данных – 110 жалоб [5]. Такую неутешительную отечественную статистику можно объяснить тем, что, несмотря на наличие правовых норм, которые регулируют обработку персональных данных в Украине, проблемным вопросом пока остается механизм их функционирования и их бланкетность.

Основательная правовая база в сфере защиты персональной информации и действенные правовые нормы позволяют Кипру оставаться одним из ведущих мировых лидеров в данной области. Обработка персональных данных в Республике Кипр регулируется Законом «Об обработке персональных данных (защиты человека)» 138(I)/2001, который вступил в силу 23 ноября 2001 года [6]. Согласно вышеуказанному закону «персональными данными» определяется вся информация, касающаяся живого субъекта данных: данные расовой или этнической принадлежности, политических убеждений, религиозных или философских убеждений, участие в ассоциациях, профсоюзах, состоянии здоровья, интимной жизни, сексуальной ориентации, а также данные, касающиеся уголовного преследования [7]. Закон применяется к данным, которые обрабатываются контролером

обработки персональных данных с постоянным местом пребывания в Республике Кипр, или в месте, где применяется законодательство Кипра в силу действия международного публичного права. Конституция Республики Кипр 1960 года устанавливает, что каждый человек имеет право на уважение его личной и семейной жизни, и запрещается любое вмешательство, за исключением условий, когда соответствующее вмешательство необходимо в интересах Республики Кипр, обеспечения конституционного порядка, общественной безопасности, общественного порядка, здоровья и нравственности населения или защиты прав и свобод, гарантированных Конституцией [8].

Ключевым субъектом контроля обработки персональных данных по законодательству Кипра является Уполномоченный по защите персональных данных (комиссар). Это публичный административно-независимый орган, основной целью которого является применение закона и обеспечение права каждого индивида на защиту личной жизни, когда обрабатываются его персональные данные. В соответствии с законодательством в сфере защиты персональных данных, действующего на территории Кипра, контроллер данных (любое лицо, которое определяет цель и средства по обработке персональных данных) обязан письменно уведомить комиссара по системе регистрации и о порядке обработки вверенных ему персональных данных [6]. В отличие от Кипра, в Украине контроль за обработкой персональных данных осуществляет Уполномоченный Верховной Рады Украины по правам человека в соответствии с Законом Украины «О внесении изменений в некоторые законодательные акты Украины относительно усовершенствования системы защиты персональных данных» от 03.07.2013 года №383-VII [9]. Заметим, что отечественное законодательство с 1 января 2014 года не обязывает владельцев регистрировать базы персональных данных. В соответствии со статьей 9 Закона Украины «О защите персональных данных» от 01.06.2010 года №2297-VI установлено, что владельцы базы персональных данных обязаны сообщить Уполномоченному об обработке персональных



данных, что представляет особый риск для прав и свобод субъектов этих данных [10]. Такой подход, безусловно, негативно повлияет на состояние защиты персональных данных, ведь уменьшение прямого контроля над оборотом и формированием баз персональных данных позволит некоторым субъектам злоупотреблять предоставленным правом.

Родственным в правовых нормах Республики Кипр и Украины является то, что общие условия обработки персональных данных не распространяются для целей выполнения налоговых обязательств, национальной безопасности, общественного порядка и уголовных расследований. Во всех остальных случаях персональные данные могут подлежать обработке исключительно при условии предоставления письменного согласия физического лица [11]. Согласие, полученное от физического лица незаконным путем или противоречащим обычаям нравственности, или нормам конкретного закона не считается таким, которое дает право на обработку персональных данных. В данном случае подвергается сомнению добровольность предоставления согласия на обработку персональных данных в трудовых отношениях на отечественных предприятиях, учреждениях и организациях, где подчиненное положение работника не всегда может действительно быть «добровольным».

Законодательство Кипра предусматривает право субъекта получить интересующую информацию при условии подачи запроса к контроллеру данных. На такой запрос контроллеры данных обязаны предоставить ответ в течение четырех недель. Контроллер данных имеет право взимать плату за каждый запрос в размере 17 евро [12]. Законодательство Украины предусматривает бесплатный доступ к персональным данным, которые были вверены владельцу персональных данных. Это является безусловным преимуществом отечественного законодательства, которое обеспечивает беспрепятственность доступа к информации для всех субъектов, данные которых попадают под процесс обработки.

Стоит отметить, что законодательство Кипра ставит высокие условия для трансграничной передачи данных

третьей стороне. Для указанной передачи данных необходимо получить письменное разрешение комиссара, которое выдается только в том случае, если комиссар будет уверен, что данные будут передаваться под надлежащим и соответствующим уровнем защиты. В частности, Комиссия Европейского Союза решила, что в соответствии со статьей 25 (6) Директивы 95/46/ЕС Швейцария, Аргентина, Канада, Остров Гернси, Остров Мэн, организации/компании в США, которые интегрированы в Safe Harbor, а также Бюро таможенного и пограничного контроля США предоставляют адекватную защиту, поэтому комиссар выдает безоговорочно лицензии на передачу данных в эти страны и организации. Также комиссар может выдать лицензию для передачи данных в страны, которые не обеспечивают адекватную защиту, при условии, если контроллер имеет достаточно гарантий по договорным условиям, что защита частной жизни и фундаментальных прав и свобод будут соблюдены. Вышеизложенный перечень свидетельствует, что Украина пока не получила мирового признания и доверия как страна, которая способна на международном уровне защищать персональные данные, вверенные для защиты. Это вызвано тем, что в Украине не предусмотрен такой основательный законодательный подход к защите персональных данных, что делает украинцев более уязвимыми, ведь национальный уровень защиты пока не соответствует мировому.

Несмотря на действенную и функциональную правовую базу института защиты персональных данных Республики Кипр, следует признать и наличие зафиксированных правонарушений по обороту таких данных. За правонарушения в сфере защиты персональных данных законодательство Кипра различает гражданскую и уголовную ответственность. Гражданская ответственность предусматривает предупреждение и установление срока для устранения нарушений, а также штраф в размере до 30 000,00 евро и временное или полное отозвание разрешения комиссара для последующей обработки данных, и/или уничтожение соответствующих данных. Уголовная ответственность заключается

в наложении судом штрафа в размере до 8 453,00 евро и лишение свободы сроком до пяти лет. Также в случае утечки персональной информации через понесенные определенные убытки физическое лицо имеет право на компенсацию от контроллера данных, за исключением случаев, когда контроллер данных не несет ответственность за такие убытки.

Как выше отмечалось, граждане направляют комиссару свои обращения о нарушении их персональных данных в форме жалоб. Однако, чаще комиссар сам инициирует собственные расследования по вопросам соблюдения законодательства в сфере защиты персональных данных. Комиссар не обладает полномочиями возбуждать уголовное производство по результатам расследований, однако он может сообщить о имеющихся правонарушениях в Управление Генерального прокурора, который ситуативно решает – нарушать уголовное производство или нет.

Самая крупная административная санкция в форме штрафа в размере 3 000,00 евро была применена комиссаром к контроллеру данных вследствие нарушения компанией раздела 4(1)(с) Закона «Об обработке персональных данных (защита человека)» (принцип пропорциональности) [6]. Компания собирала и обрабатывала большой объем персональных данных, чем это было необходимо. Также был случай, когда комиссар наложил штраф в размере 2 562,00 евро на компанию, которая нарушила нормы законодательства в сфере защиты персональных данных, в частности: нормы о порядке обработки персональных данных в целях прямого маркетинга путем отправки рекламных текстовых сообщений без предварительно полученного письменного согласия физического лица. Штраф в размере 2 562,00 евро был наложен на директора фирмы за нарушение норм, регулирующих порядок обработки чувственных персональных данных.

Особого внимания заслуживает дело, которое рассматривалось в 2013 году с участием Центрального банка Кипра и его работников. Сотрудники банка обратились с заявлением к комиссару о несанкционированном размещении новых камер видеонаблю-



дения на территории здания банка. В ходе осмотра было обнаружено, что о монтаже 4 из 80 камер работниками службы безопасности были проинформированы другие сотрудники банка в устной форме. Также отсутствовали знаки предостережения о наличии камер видеонаблюдения в помещении банка. Информация, содержащаяся на сайте в сети Интернет, по размещению видеосистем на территории банка во внимание не принималась, ведь это не является предупреждением о проведении сбора персональных данных в установленном законодательством порядке. По результатам рассмотрения дела комиссар вынес предостережение относительно действий руководства и службы безопасности банка [13].

Первый уголовный процесс, который был начат за нарушение законодательства Кипра в сфере защиты персональных данных и частной жизни касался владельца массажного салона, в котором были скрыто размещены видеокамеры без ведома и предварительного согласия клиентов и сообщения комиссара. По результатам рассмотрения материалов дела, суд вынес решение в виде лишения свободы владельца салона сроком на три месяца. Самый длительный срок лишения свободы составляет 16 месяцев, который был вынесен лицу вследствие его несанкционированного доступа к персональным данным физических лиц с целью получения доступа к кредитным картам третьих лиц с целью использования чужих средств.

Юридическая ответственность за правонарушения в сфере защиты персональных данных в Украине предусмотрена статьями 188-39, 188-40 Кодекса Украины об административных правонарушениях в форме финансовой санкции в размере от 1 700,00 грн. до 17 000,00 грн. [14], ст. 182 Уголовного кодекса Украины в форме финансовой санкции от 8 500,00 грн. до 17 000,00 грн., исправительных работ на срок до 2 лет, ареста до 6 месяцев, ограничение свободы сроком от 3 до 5 лет и лишение свободы на тот же срок [15]. Стоит заметить, что санкции вышеуказанных статей достаточно приближены к тем, которые предусмотрены законодательством Республики Кипр, что, в свою очередь, свидетельствует о верно выбранном курсе раз-

вития отечественной законодательной базы.

Стоит заметить, что впервые в Украине факт привлечения к ответственности за нарушение законодательства в сфере защиты персональных данных был изложен в постановлении Подольского районного суда города Киев от 07.02.2013 года по делу №758/1119/13-п. Суд признал виновным директора ООО «Издательство «Ридерз Дайджест» в совершении правонарушения, предусмотренного ч. 2 ст. 188-39 Кодекса Украины об административных правонарушениях – неуведомление или несвоевременное уведомление об изменении сведений, предоставляемых для государственной регистрации базы персональных данных, за что был наложен штраф в размере 3 400,00 грн. [16]. Примером привлечения к уголовной ответственности за несанкционированное раскрытие персональных данных в Украине путем раскрытия данных третьему лицу с использованием служебного положения является дело №592/12270/13-к. По результатам рассмотрения материалов дела Ковпаковский районный суд города Сумы 18.11.2013 года вынес приговор, которым признал лицо виновным в совершении уголовного преступления, предусмотренного ч. 1 ст. 361-2 Уголовного кодекса Украины, и назначил наказание в виде 2-х лет лишения свободы [17].

Вышеприведенные судебные дела и уменьшение количества обращений граждан Кипра свидетельствуют об имеющемся диалоге «государство – закон – личность», ведь развитая правовая база и действенный механизм ее применения является залогом успеха в построении здоровых правоотношений в обществе. К сожалению, несмотря на динамичный темп разработки правовой базы Украины в области защиты персональных данных, степень защиты персональных данных фактически остается на низком уровне, о чем свидетельствует высокое количество обращений граждан и имеющиеся судебные решения. Однако, наличие только правовых норм без стабильного диалога со стороны государства, препятствует Украине развиваться и позиционировать себя сильным субъектом на международ-

ной арене, в частности, в сфере защиты персональных данных. Стоит признать, что Украина только начала свой путь по защите персональных данных. С целью предотвращения совершения правонарушений и снижения количественного показателя обращений граждан за нарушения их прав, необходимо налаживать конструктивный диалог с государством. Действенным механизмом может стать проведение информационных кампаний и активной просветительской работы для граждан не только государственными учреждениями, но и субъектами хозяйствования частного сектора.

Выводы. Опыт Республики Кипр доказал, что именно систематическая работа комиссара обеспечивает полную осведомленность лиц относительно их прав на персональные данные. Именно осведомленность человека сможет помочь предотвратить и избежать огласки или несанкционированного распространения персональных данных перед третьими лицами. По нашему мнению, необходимо на национальном уровне развивать и популяризировать проведение мероприятий информационно-разъяснительного характера среди населения, а также непосредственно на базе предприятий, учреждений и организаций. С этой целью должна быть разработана государственная программа по правовому образованию населения, по которой систематически должны организовываться и проводиться ряд бесплатных семинаров для физических и юридических лиц с целью предоставления практических рекомендаций по применению законодательства в сфере защиты персональных данных. Государство в лице Уполномоченного по правам человека во взаимодействии с руководителями предприятий, учреждений, организаций, а также институтами гражданского общества в соответствии с положениями п. 6, 7, 11 статьи 23, статьи 26 Закона Украины «О защите персональных данных» должны принимать в соответствии с законодательством меры для обеспечения прохождения ответственным работником обучения в сфере предотвращения и противодействия незаконному обороту персональных данных. Систематическое повышение квалификации ответственного работ-



ника не реже одного раза в год путем прохождения обучения на базе соответствующего учебного заведения, которое принадлежит сфере управления специально уполномоченного органа или на базе предприятия, учреждения, организации.

Именно общее дело и цель преодолеть трудности в процессе становления и функционирования нового правового института для нашего государства является решающим и действенным шагом на пути к построению правового государства с мировым авторитетом.

Список использованной литературы:

1. Статистические данные Государственной службы статистики Украины относительно прямых иностранных инвестиций (акционерный капитал) из стран мира в экономику Украины по результатам 2013 года. [Электронный ресурс] – Режим доступа: <http://www.ukrstat.gov.ua/>.
2. Protection of personal data in Cyprus is at a high level, says Commissioner. [Электронный ресурс] – Режим доступа: <http://famagustagazette.com/protection-of-personal-data-in-cyprus-is-at-a-high-level-says-commissione-p17882-69.htm>.
3. Информация об обращениях граждан к Уполномоченному Верховной Рады Украины по правам человека в 2010 году. [Электронный ресурс] – Режим доступа: http://www.ombudsman.gov.ua/ru/index.php?option=com_content&view=category&layout=blog&id=128&Itemid=45.
4. Отчет о выполнении Государственной службой Украины по вопросам защиты персональных данных задач в 2012 году. [Электронный ресурс] – Режим доступа: <http://zpd.gov.ua/dszpd/uk/publish/category/38951>.
5. Подведение итогов работы Государственной службы Украины по вопросам защиты персональных данных в 2013 году. [Электронный ресурс]. – Режим доступа: <http://zpd.gov.ua/dszpd/uk/publish/category/38951>.
6. Γιάννος Δανιηλίδης «28η Ιανουαρίου – Ημέρα Προστασίας Προσωπικών Δεδομένων» 23/01/2014. [Электронный ресурс]. – Режим доступа: <http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/4692F7E7895216A1C2257C690041D1B7?OpenDocument>.
7. Linklaters: Data Protected (Cyprus). [Электронный ресурс]. – Режим доступа: <https://clientsites.linklaters.com/Clients/dataprotected/Pages/Cyprus.aspx>.
8. The Constitution of the Republic of Cyprus. [Электронный ресурс]. – Режим доступа: http://presidency.gov.cy/.../CY_Constitution.pdf.
9. О внесении изменений в некоторые законодательные акты Украины относительно усовершенствования системы защиты персональных данных: Закон Украины от 03.07.2013 года №383-VII // Ведомости Верховной Рады (ВВР), 2014, № 14, Ст. 252.
10. О защите персональных данных: Закон Украины от 01.06.2010 года № т2297-VI // Ведомости Верховной Рады Украины. – 2010. – № 34. – Ст. 481.
11. Data Protection & Privacy – Jurisdictional Comparisons: Cyprus. Andreas Neocleous & Co LLC, Nicholas Ktenas & Chrystalla Neophytou. [Электронный ресурс] – Режим доступа: <http://www.sweetandmaxwell.co.uk/Catalogue/ProductDetails.aspx?recordid=4846&searchorigin=European+lawyer+reference&productid=556041>.
12. Giannos Danielidis Personal Data, 12.12.2012. [Электронный ресурс] – Режим доступа: <http://www.cypruslawdigest.com/topics/personal-data/item/169-personal-data>.
13. Commissioner For Personal Data Protection (Cyprus). Annual Report 2009, Nicosia, July 2010. [Электронный ресурс] – Режим доступа: [http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/697e70c0046f7759c2256e8c004a0a49/f8e24ef90a27f34fc2256eb4002854e7/\\$FILE/annual%20report%202009%20eng.pdf](http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/697e70c0046f7759c2256e8c004a0a49/f8e24ef90a27f34fc2256eb4002854e7/$FILE/annual%20report%202009%20eng.pdf).
14. Кодекс об административных правонарушениях в Украине от 07.12.1984 г. // Ведомости Верховного Совета Украинской ССР (ВВР) 1984, приложение к № 51, с.1122.
15. Уголовный кодекс Украины от 05.04.2011 года № 2341-III // Ведомости Верховной Рады Украины (ВВР). – 2001. – № 25-26. – Ст. 131.
16. Постановление Подольского районного суда города Киев от 07.02.2013 г. по делу № 758/1119/13-п. [Электронный ресурс] – Режим доступа: ЛИГА.Закон.
17. Приговор Ковпаковского районного суда города Киев от 18.11.2013 г. по делу № 592 / 12270/13-к. [Электронный ресурс] – Режим доступа: ЛИГА.Закон.